Notice of Allowability	Application No.	Applicant(s)	
	09/818,567	FURUYA ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed 28 June 2006 and Telephonic Communication on 8 August 2006*.

2. ☒ The allowed claim(s) is/are *1-13 (renumbering as 9-12, 21-24,38, and 33-36 respectively)*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☒ Certified copies of the priority documents have been received in Application No. *09/784,254* .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 28 June 2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *8 August 2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

JACQUES LOUIS JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Reasons for Allowance

1. In response to amendment filed on 28 June 2006 and Examiner Initiated Interview on 8 August 2006. The IDS submitted 28 June 2006 has been considered.

2. The terminal disclaimer filed on 28 June 2006 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of co-pending application Serial No. 09/784,254 has been reviewed and is accepted. The terminal disclaimer has been recorded.

3. An examiner's amendment to the record is attached. Please enter entire claim set. The attached amendment corrects error within the independent claims. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment to amend claims 9, 21, and 33; was authorized by attorney of record Carl I. Brundidge in phone Interview initiated by Examiner on 8 August 2006.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance: Claims 9-12, 21-24, 33-36, and 38 are allowed due to amendment and arguments presented on 2 December 2005 beginning on page 15, that in the reference 'the decryption operation is a different order and combination than the claimed invention, the reference consist of one round of an XOR3 operation, a shuffle operation, and an XOR1 operation whereas the claimed invention 1st operation uses a feedback back value from the result of order cipher text value which utilizes two

random numbers which are generated in complete isolation from any of said plurality of cipher text blocks'.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen. Tran
Patent Examiner
Technology Center 2134
31 July 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

Claims 1-8 (canceled).

9. (currently amended) A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a ~~the~~ series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext ~~ciphertext~~ obtained from the ciphertext ~~plaintext~~ has been altered,

wherein one of said decryption operations for producing a ~~the~~ plaintext block i corresponding to a ~~the~~ ciphertext block i ($2 \leq i \leq$ a number of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block

corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or ~~of~~ said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

10. (previously presented)The symmetric-key decryption method as claimed in claim 9, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext blocks.

11. (original) The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

12. (previously presented)The symmetric-key decryption method as claimed in claim

11, further comprising steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claims 13-20 (canceled).

21. (currently amended) A symmetric-key decryption apparatus comprising:

a circuit for dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating a ~~the~~ series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

a circuit for examining the redundancy data to detect whether the plaintext ~~ciphertext~~ obtained from the ciphertext ~~plaintext~~ has been altered,

wherein said decryption operation circuit for producing a ~~the~~ plaintext block i corresponding to a ~~the~~ ciphertext block i ($2 \leq i \leq$ a number of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation.

22. (previously presented)The symmetric-key decryption apparatus as claimed in claim 21, wherein said random number generation circuit divides a random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said ciphertext blocks.

23. (original) The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. (previously presented)The symmetric-key decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data.

Claims 25-32 (canceled).

33. (currently amended) A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to perform the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a ~~the~~ series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext ~~ciphertext~~ obtained from the ciphertext ~~plaintext~~ has been altered,

wherein one of said decryption operations for producing a ~~the~~ plaintext block i corresponding to a ~~the~~ ciphertext block i ($2 \leq i \leq$ a number of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or ~~of~~ said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

34. (previously presented)The medium storing a program as claimed in claim 33, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said

ciphertext block.

35. (original) The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. (previously presented)The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claim 37 (canceled).

38. (previously presented)The symmetric-key decryption apparatus as claimed in claim 22, wherein said random number generation circuit further comprises:

a pseudorandom number generator for generating said random number sequence based on said secret key; and

a circuit for producing said random number blocks from said random number sequence.